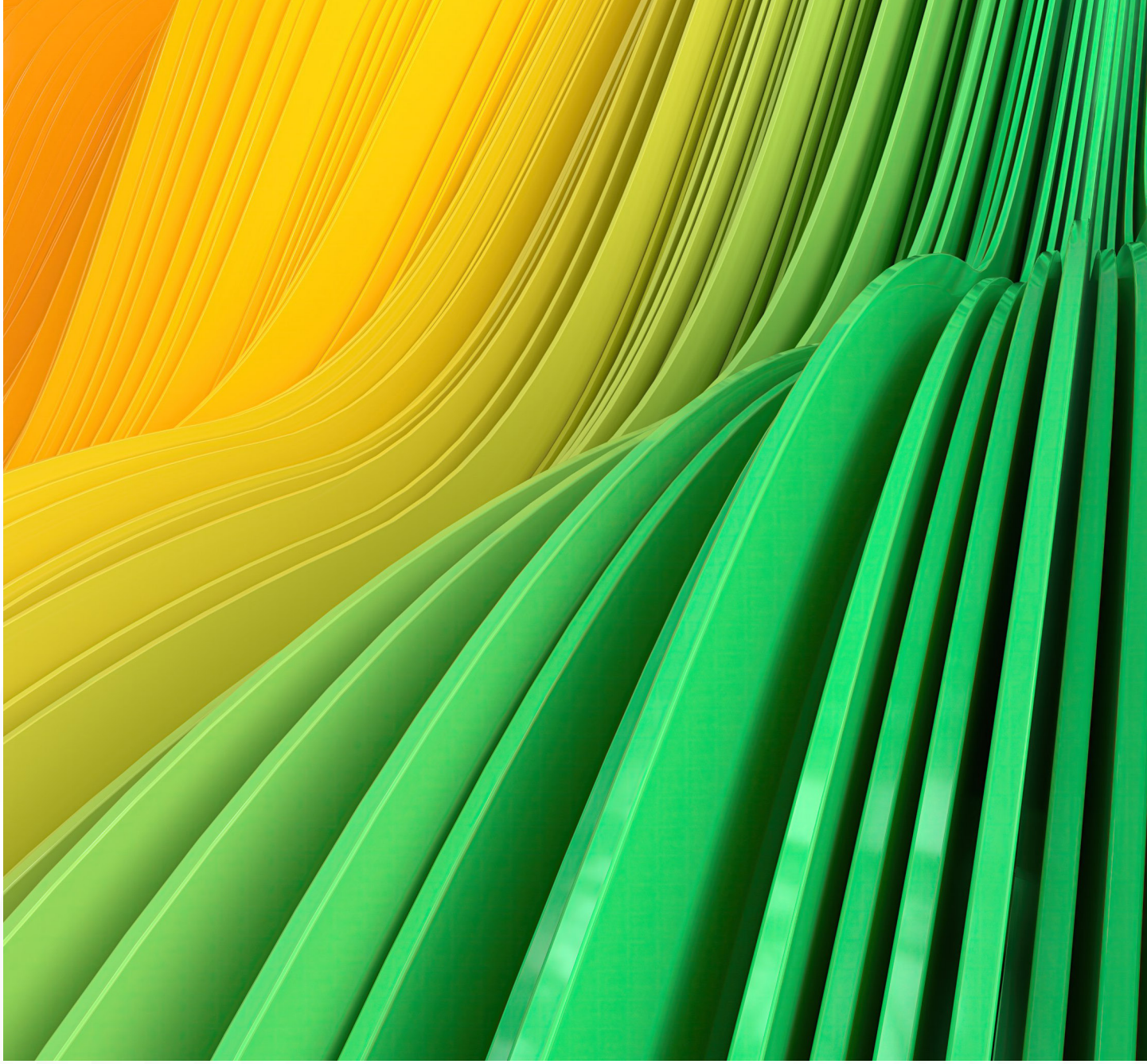


ラテラルムーブがせっかくのSASEを台無しに!

多層防御の最終防衛ラインとなる キャンパスの守り方、教えます

HPE aruba networking

Contents

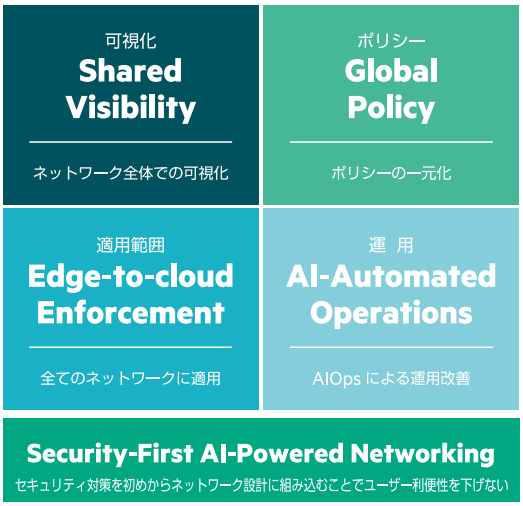
キャンパスネットワーク編

セキュリティがビルトインされた Security-First AI-Powered Networking

SaaSをはじめとした各種クラウドアプリケーションを業務利用する機会が一般化した今、快適な業務環境を提供するためには、利便性や体感、快適さといったユーザエクスペリエンス（UX）を向上させるネットワークの最適化は重要な役割を果たします。一方で、ランサムウェアをはじめとする高度な脅威によるビジネス被害の拡大は後を絶ちません。特に、企業規模を問わずマルウェア被害が相次いでいることからも、どんな企業であってもセキュアな環境づくりがこれまで以上に求められています。

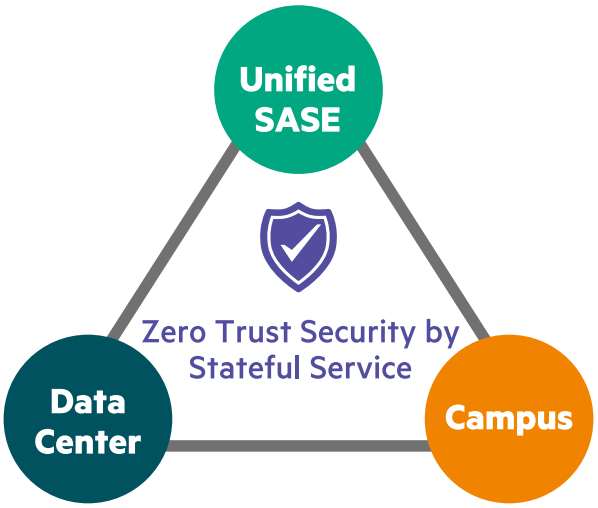
ただし、ネットワークの利便性と強固なセキュリティに求められる要件は、相反するものになりがちです。快適にアプリケーションを利用するためにネットワークへのアクセスを容易にすれば利便性は高まりますが、コンプライアンスの遵守を含めたセキュリティの観点からは、トラフィックや振る舞いの可視化、接続時の認証・認可、権限に応じたアクセス制御などが必要になり、要求レベルを高めるほど、ネットワークの性能や使い勝手に影響を与えてしまい、結果としてUXの低下を招くことになってしまいます。

そこでHPE Aruba Networkingが掲げているのが、最適なUXを維持しながらセキュアなネットワークを実現するためのアーキテクチャである「Security-First AI-Powered Networking」です。Security-First AI-Powered Networkingには、「ネットワーク全体での可視化」「ポリシーの一元化」「Edge-to-Cloud の全てのネットワークに適用」「AIOpsを活用したセキュリティの向上と運用の改善」という4つの特長が備わっています。



セキュリティの機能を標準でネットワーク製品にビルトインさせるSecurity-First AI-Powered Networkingによって、ハイパフォーマンスで快適なネットワークと高度な脅威に対応できるセキュアなネットワークを同時に提供することが可能となるのです。

セキュリティがビルトインされたネットワークは、多くの企業が検討を進めるゼロトラストのコンセプトにつながります。なかでも重要な要素となるのが、ステートフルサービスです。具体的には、内部からの必要な通信のみ許可し、外部からの不明な通信を全てブロックするステートフルファイアウォール機能です。キャンパスやWAN（=Unified SASE）、そしてデータセンターなど企業を取り巻くネットワーク全ての領域でステートフルサービスを実装し、セキュリティと利便性を兼ね備えたネットワークを実現します。

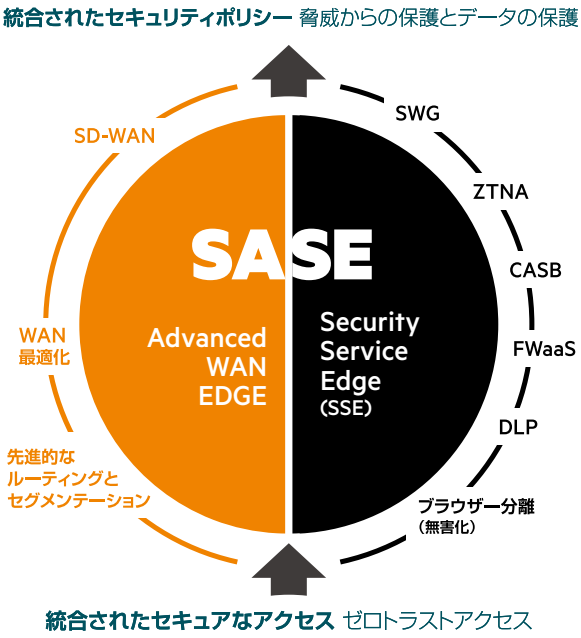


ゼロトラストを具現化するSASE

そもそもゼロトラストとは、ネットワークやセキュリティにおいて「何も信頼しない」ことを前提とした考え方です。この信頼しないという考え方に立つゼロトラストでは、ネットワークに接続してくるデバイスやユーザーが、常に信頼に足るかどうかをその都度判断していくことが必要で、何か問題があれば動的に対処できる仕組みづくりが重要です。また、昨今では標的型攻撃も含めた高度化された脅威の広がりとともに、従業員が機密情報を持ち出す内部不正といったインシデントも発生するなど、外部からの脅威だけでなく、境界内部にも脅威が存在してしまっています。その意味では、侵入されることを前提とした多層防御セキュリティの考え方にシフトせざるを得なくなっていることも、ゼロトラストの重要性が高まる大きな要因の1つといえるのです。

このゼロトラストを実現するための環境として注目されているのが、統合ネットワークとセキュリティ機能の各種コンポーネントを組み合わせたSASE（Secure Access Service Edge）です。SASEは、大きく分けて統合セキュリティ機能を備えたSSE（Security Service Edge）と、SD-WANを中心としたWANエッジサービスの2つが備わっています。

SSEには、クラウドセキュリティとしてプロキシ機能やフィルタリング機能を提供するクラウドSWG（Secure Web Gateway）やプライベートゾーンへのアクセスを制御することが可能なZTNA（Zero Trust Network Access）、クラウドサービスにおける利用状況の可視化や制御を行うCASB（Cloud Access Security Broker）、アクセス制御をはじめとした高度な次世代ファイアウォール機能がサービス実装できるFWaaS（Firewall as a Service）、重要データの漏洩などを防ぐDLP（Data Loss Prevention）などを組み合わせて、単一のセキュリティサービスとして提供するものです。

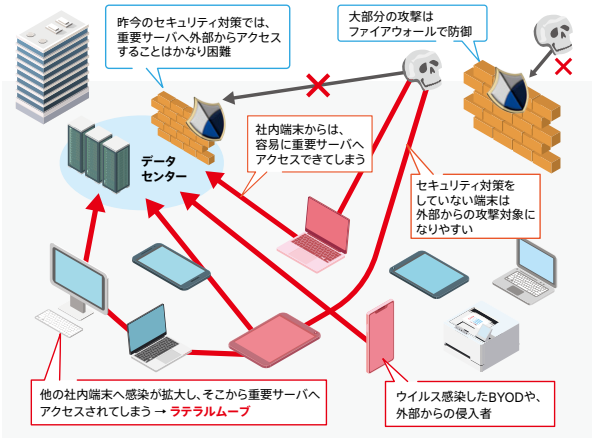


また、エンドポイントそのものを防御するための仕組みとして注目されているのが、デバイスの挙動を監視して保護することが可能なEDR（Endpoint Detection and Response）や、PCやスマートフォン、タブレットなどあらゆるデバイスを管理することが可能なUEM（Unified Endpoint Management）などです。多くの企業が従来型のアンチウイルスソフトに代わってEDRを検討・導入する傾向にあり、自社で管理できるエンドポイント保護には有効な策となるはずです。

ゼロトラストを加速させるランサムウェア、ラテラルムーブが大きな脅威に

そんなゼロトラストを実践する動きを加速させているのが、端末のロックやデータの暗号化によってシステムの業務利用を妨害し、復旧と引き換えに金銭を要求するランサムウェアによる被害拡大です。ランサムウェアは、システムや企業規模の大小に関わらずその被害が報告されており、特定の大企業だけを狙った攻撃ではないことからも、多くの企業での対策が求められます。ランサムウェアは、メールやWebサイトからの感染とともに、脆弱性によるネットワーク経由や公開サーバへの不正ログインなど、その感染経路や方法は多種多様です。

近年は、マルウェアを添付したメールを機械的にばらまくのではなく、攻撃者自身が企業を直接標的にし、企業や組織のネットワークへひそかに侵入したうえで、侵害範囲拡大などを行う人手によるランサムウェア攻撃が増えています。この場合、EDRをはじめとしたデバイスのセキュリティやファイアウォールなどのゲートウェイセキュリティを突破し、企業のイントラネット内に侵入して被害範囲を拡大させます。イントラネットとしてのセキュリティ対策が十分でない場合、他の社内端末へ感染が拡大し、そこから重要サーバへアクセスされてしまう“ラテラルムーブ”が起こり、より被害を拡大させてしまうことになるのです。



実は、IDaaS（Identity as a Service）やSWGをはじめクラウド側に認証基盤や境界防御の機能を持たせるゼロトラストですが、イントラネットに侵入された後の対策については、十分カバーできていません。既設のファイアウォールやUTM（Unified Threat Management）といったゲートウェイ型のソリューションやEDRなど新たなエンドポイント対策を進めている企業は少なくありませんが、侵入後に発生するラテラルムーブへの対策とはなりづらいところです。せっかく複数コン

ポーネントを組み合わせたSASEによる多層防御を整備したとしても、一度侵入されてしまえば被害を防ぐことは難しいものです。ラテラルムーブによって、せっかく整備したSASEが台無しにされてしまうことにもなりかねないのです。

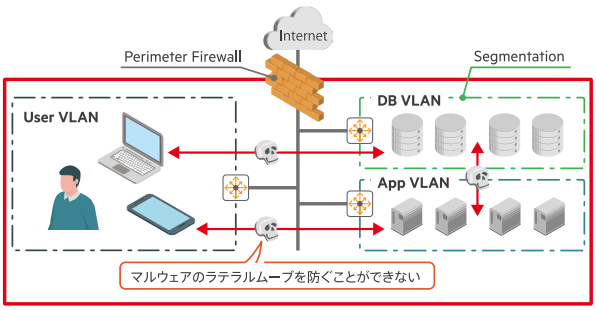
ラテラルムーブに有効な Micro Perimeter & Micro Segmentation

ではどんな対策が必要なのでしょうか。具体的には、Micro PerimeterとMicro Segmentationという2つのアプローチを検討することが有効です。

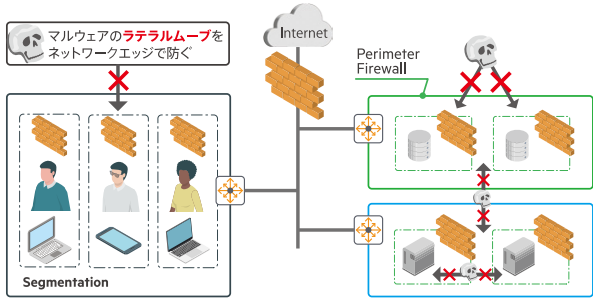
Micro Perimeterとは、インターネットとの境界に設置していたファイアウォールを、部門や部署など細かな範囲に設置したり機能実装したりするもので、境界防御を至るところに設けることで、マルウェアの横展開を最小限におさえることができます。

Micro Segmentationは、部署や利用者ごとにロールを割り当て、最小限のアクセスだけを許可するアプローチです。万一デバイスがマルウェアに感染したとしても、最小限のアクセスしか許可されていないことで、ラテラルムーブをおさえることが可能です。最近ではネットワークカメラやRaspberry Piを使ったデバイスなど、IoT機器を攻撃の起点にする脅威も出てきていることから、IoT機器についてもどのようにセグメンテーションするのか考える必要があります。

■ Legacy Perimeter & Segmentation



■ Micro Perimeter & Micro Segmentation



多くの境界を設置してアクセスできる範囲を最小限にしておくMicro PerimeterとMicro Segmentationは、イントラネットへの有効なセキュリティ対策となってくるわけです。

キャンパスネットワークに求められること

ここで、企業を取り巻くネットワークの1つであるキャンパスにおいて、Micro PerimeterとMicro Segmentationはどのように実践していくべきなのでしょうか。そもそも営業所や支店といったキャンパスネットワークにおいては、PCをはじめとしたエンドポイントが無線LANを経由してネットワークに接続し、本社はVPNなどを用いた閉域ネットワークで行い、インターネットにブレイクアウトする回線も有しています。特に拠点数が多くなればなるほど、既存で利用しているネットワークを大きく刷新するようなアプローチは大きな費用が発生してしまい、投資判断が難しいケースも出てきます。

できれば、既存環境を維持したまま、ユーザーごとにロールを割り当ててアクセス範囲を最小限にするMicro Segmentationの環境が整備できるものが望ましいでしょう。VLANを細かく設定してネットワークへの影響範囲を最小限にすることも重要ですが、マルウェアを検知した際に特定のデバイスを隔離していくような、柔軟性を持った運用が可能なDynamic Segmentationによるアプローチが望ましいところです。

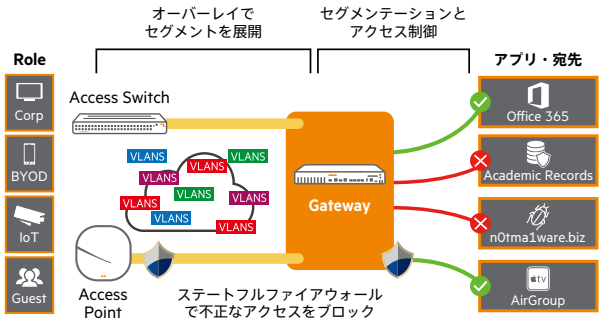
また、パケットの振る舞いを検証して動的にフィルタリングが可能なステートフルファイアウォールをできる限り細かな範囲に設置することで、Micro Perimeterとしての環境整備を行っていきます。その場合、エンドポイントに導入しているEDRを活用すれば、確かにファイアウォールとしての役割は果たしますが、いわゆるIoT機器などEDRのエージェントが導入できないものへの対策も必要です。できれば、IoT機器をはじめとしたエージェントレスなデバイスに対応できるよう、エッジ側で集約できるような環境を検討したいところです。

Security-First AI-Powered Networkingによるキャンパスのゼロトラスト

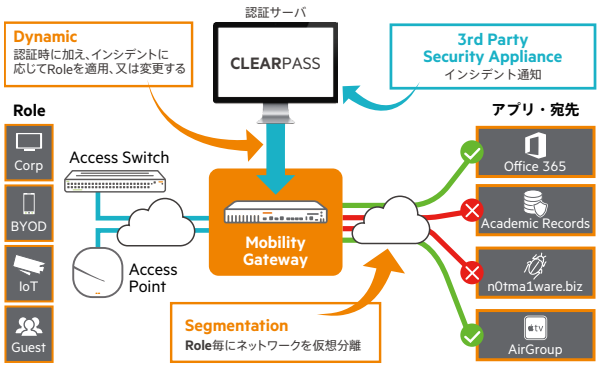
ここで有効になってくるのが、HPE Aruba Networkingが提供するイントラネットセキュリティです。基本的な考え方としては、キャンパスやブランチ、そしてデータセンターなどの領域においても、ネットワークエッジでマルウェアのラテラルムーブを防ぐという考え方です。

すでに稼働中のネットワークのセグメントを細かく切っていくのは難しいため、HPE Aruba Networkingではネットワークのコアスイッチの横にモビリティ・ゲートウェイ／コントローラーを設置し、エッジにあるLANスイッチやアクセスポイントとの間でオーバーレイによるトンネルを張ることで仮想ネットワークを構築します。既存環境を変更することなく新しいセグメントが設定できます。

また、モビリティ・ゲートウェイ／コントローラーはステートフルファイアウォール機能を実装しており、オーバーレイネットワークに接続された端末ごとにファイアウォールを設置したかのような環境をつくり出すことが可能です。



キャンパスの場合、ユーザーの役割が変更する機会が多いだけでなく、最初に認証した後からマルウェアに感染してしまうといった端末の状態変化が激しいものです。HPE Aruba Networkingでは、認証サーバとなるClearPassを設置し、端末やユーザーの認証を行ってネットワークの接続を許可します。万一その端末がマルウェアに感染したということをファイアウォールやUTMで検知した場合、その通知をもとにセッションを維持しているClearPassがその端末を別のセグメントに移動させるといった、動的な制御が可能になります。3rd Partyのセキュリティ製品と連携することで、検知から隔離までの処理が半自動化でき、ラテラルムーブの被害を最小限におさえることが可能なDynamic Segmentationを実現します。



実はSecurity-First AI-Powered Networkingにおけるキャンパス領域で実現するMicro PerimeterおよびMicro Segmentationの環境づくりは、利便性とセキュリティ性を兼ね備えた数万台のデバイスを結ぶネットワークを持つ米国国防総省（ペンタゴン）にも採用、導入されています。有線スイッチから無線LAN、モビリティ・ゲートウェイ／コントローラー、そしてDynamic Segmentationを実現するための認証サーバとなるClearPassも導入しており、強固なネットワークセキュリティを維持しながら、快適なネットワーク環境の整備を実現しています。

キャンパスネットワークに必要なオーバーレイネットワークによるDynamic Segmentationが、ラテラルムーブによるマルウェア被害を最小限におさえるためのイントラネットセキュリティには有効です。Security-First AI-Powered Networkingにおけるキャンパス向けソリューション、ぜひ一度ご検討してみてはいかがでしょうか。

お問い合わせ : 日本ヒューレット・パッカード合同会社　www.arubanetworks.com/contact